IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Kevin R. Driscoll	Examiner: Fikremariam Yalew
Serial No.:	10/750,529	Group Art Unit: 2136
Filed:	December 31, 2003	Docket No.: H0005071.35998
Title:	DATA AUTHENTICATION AND TAMPER DETECTION	

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

In response to the Office Action mailed November 4, 2008. No amendments are submitted with this Request, which is filed with a Notice of Appeal for the reasons stated below.

§102 Rejection of the Claims

Claims 1-8 and 13-31 were rejected under 35 U.S.C. § 102(e) for anticipation by Grawrock et al. (hereinafter referred to as Grawrock) U.S. Patent No. 2002/0080974 B2. Among the differences, claim 1 recites "performing data authentication, wherein performing the data authentication comprises generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value." Claim 13 includes a similar limitation.

In the Response to Arguments section, the Office indicated that Grawrock teaches generating a digital signature based on an ephemeral value at 0028-0029, 0034 and steps 310, 315 in Fig. 3. Applicant respectfully traverses. Grawrock at 0028-0029 relates to a digital signature. However, this digital signature is not signed with a key that is equal to an ephemeral value. In contrast, this digital signature is signed "with a private key (CAPRK) of a certification authority . . ." Grawrock at [0028]. In Grawrock, the CAPRK is not defined as an ephemeral value. Rather, the EUPUK and the EAPRK are keys that are equal to an ephemeral value. Grawrock at 0034 relates to performing a hash operation "on the EAPUK. . .", not using the EAPUK to perform the hash. In other words, the EAPUK is data that is being hashed. Grawrock at steps 310 and 315 of Fig. 3 relate generally to ephemeral keys (EAPUK and EAPRK). However, this section of Grawrock does not disclose generating a digital signature using a key that has a value equal to an ephemeral value.

Further, the Office alleges that performing encryption is equivalent to generating a digital signature or hash:

> Further more the system in Grawrok (sic) relates to use of ephemeral value as a cryptographic key to perform encryption/decryption of data(i.e., the examiner reasonably interpreted using ephemeral value as a cryptographic key to perform encryption equivalent to use of an ephemeral value as a cryptographic key generate a digital signature or hash).

Office Action at page 2.

Applicant respectfully traverses. Encryption does not equal digital signature generation. Encryption is a reversible operation used to protect the data. Digital signature generation is used to authenticate the data. Protection does not equal authentication (as recited in claims 1, 5, 13, 24 and 28). For example, among the differences, claim 1 recites "performing data authentication, wherein performing the data authentication comprises generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value." (emphasis added).

Further, in the Response to Arguments section, the Office indicated that Grawrock teaches performing data authentication at steps 325 and 330 of Fig. 3 (regarding the description of "validate identify using identify credential."). Office Action at page 3. In Grawrock, the identity credential relates to "(i) secret data associated with the identity (e.g., a permanent asymmetric public key of the identity, referred to as the "identity public key") and (ii) a first sequence of alphanumeric characters (e.g., a statement "TCPA Subsystem Identity")." Grawrock at [0028]. This credential is "digitally signed with a private key (CAPRK)." As noted above, in Grawrock, the CAPRK is not defined as an ephemeral value. Rather, the EUPUK and the EAPRK are keys that are equal to an ephemeral value. Therefore, Grawrock does not disclose data authentication comprising generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value.

Because Grawrock does not disclose all of the claim limitations, Applicant respectfully submits that the rejection of claims 1, 5, 13, 24 and 28 under 35 USC § 102 has been overcome. Because claims 2-4, 6-8, 14-19, 25-27 and 29-31 depend from and further define claims 1, 5, 13,

24 and 28, respectively, Applicant respectfully submits that the rejection of claims 2-4, 6-8, 14-19, 25-27 and 29-31 under 35 USC § 102 has been overcome.

§103 Rejection of the Claims

Claims 9-12 and 32-35 were rejected under 35 USC § 103(a) as being unpatentable over Johnson, P.K. et al. (hereinafter referred to as Johnson) (WO 00/18162) in view of Grawrock et al. (hereinafter referred to as Grawrock) US Patent No. 2002/0080974 B2. Applicant respectfully traverses. Neither Johnson nor Grawrock (alone or in combination) discloses or suggests all of the claim limitations.

Among the differences, claims 9 and 32 recite "generating a second digital signature with a cryptographic key having a value that is equal to the random number." In the Response to Arguments section, the Office indicated that Grawrock teaches this limitation at 0033-0034 and Fig. 5 steps 530, 540. Applicant respectfully traverses. These section of Grawrock relate to performing a hash operation "on the EAPUK. . .", not using the EAPUK to perform the hash. Further, Applicant respectfully submits that there is no suggestion to modify Grawrock to generate a digital signature. In contrast, in order to be operative, Grawrock requires encryption/decryption of the data using a cryptographic key having a value that is equal to a random number such that the data can be reproduced so that the static markers can be verified. In contrast, claims 9 and 32 recite the generating of a digital signature with such a cryptographic key. However, as noted above, the digital signature cannot be used to reproduce the encrypted data. Rather, the digital signature is used to authenticate.

Because neither Johnson nor Grawrock (alone or in combination) discloses or suggests all of the claim limitations, Applicant respectfully submits that the rejection of claims 9 and 32 under 35 USC § 103 has been overcome. Because claims 10-12 and 33-35 depend from and further define claims 9 and 32, respectively, Applicant respectfully submits that the rejection of claims 101-2 and 33-35 under 35 USC § 103 has been overcome.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (612) 373-6972 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6972

Date 2-4-2009 By

Bradley A. Forrest
Reg. No. 30,837

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Mail Stop RCE, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 4th day of February 2009

Dawn M Rose

Name

Signature